REMARKS

Claims 1-3, 7, 11-16, 18, 20-33, and 35-43 are currently pending in the subject application and are presently under consideration. Claims 11, 15, 20, 29, and 40 have been amended as shown on pages 2-9 of the Reply. New claims 44 and 45 have been added.

Applicant's representative thanks Examiner Augustin for the courtesies extended during the telephonic interview conducted on October 9, 2008. During the interview, applicant's representative clarified a number of features set forth in the claims, including the oversight capability and corruption monitoring functionality provided by the present invention. The Examiner asked that the Reply include references to the specification supporting these features, and indicated that the features would be given further consideration in light of the explanations provided during the interview.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-4, 6-18, 20-33, and 35-43 Under 35 U.S.C. §103(a)

Claims 1-4, 6-18, 20-33, and 35-43 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Christiano (US 5,671,412), in view of Rivera, *et al.* (US 6,056,786). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Christano and Rivera, *et al.*, individually or in combination, do not teach or suggest all aspects of the subject claims.

> A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning. See *KSR v. Teleflex*, 550 U.S. ___, 127 S. Ct. 1727 (2007) citing Graham v. John Deere Co. of Kansas City, 383 U. S. 1, 36 (warning against a "temptation to read into the prior art the teachings of the invention in issue" and instructing courts to "'guard against slipping into the use of hindsight'" (*quoting Monroe Auto Equipment Co. v. Heckethorn Mfg. & Supply Co.*, 332 F. 2d 406, 412 (CA6 1964))).

The subject claims relate to a license enforcement system that stores digital licenses associated with computer applications in a secure license store. A monitoring component can monitor the stored licenses and the licensed applications for user violations of the license agreements; for example, detecting when the number of current license users exceeds the agreed maximum number of users. An enforcement policy can be implemented that initiates corrective action when a violation is detected. Such corrective action can include, but is not limited to, transmitting warning messages to users or system administrators, or disabling the application whose license is being violated. To ensure that the licenses are being monitored at all times, an oversight component can observe the monitoring component to ensure its correct function. When it is determined that the monitoring component has stopped functioning, the oversight component can attempt to restart the monitoring. If the attempt to restart the monitoring component fails, the oversight component can disable the associated application to prevent license violations (see paragraph [0051] of the specification). In particular, independent claim 1 recites, *an oversight component that observes the monitoring component and the enforcement component to ensure that they have not been deactivated, wherein the oversight component restarts the monitoring component when it stops operating, and shuts down the application when the monitoring component cannot be restarted.*

Christiano does not disclose such oversight functionality. Christaino relates to a license management system that allows client computers to check out application licenses from a license server. The system monitors for violations of license policies, and takes corrective actions when a violation is detected according to a pre-determined level of enforcement. It is noted that the present Office Action merely presents the same arguments verbatim as were presented in the previous Office Action dated February 27, 2008, and does not directly address the claim amendments submitted in the reply to that Office Action, which included the above-mentioned oversight component. It is therefore reiterated that Christiano does not disclose an oversight component that ensures correct monitoring of license policies, that additionally attempts to restart monitoring when it is determined that the monitoring has stopped, and that shuts down applications associated with the license when the failed monitoring cannot be restarted. Although Christiano teaches that a license server can determine when a license violation takes place on a client computer with respect to a licensed application, the cited reference makes no allowance for oversight functionality over this usage monitoring, nor the steps disclosed in independent claim 1 to be taken when policy monitoring fails.

Rivera, *et al.* is also silent regarding such an oversight component. Rivera, *et al.* relates to a monitoring system that determines the number of concurrent users transacting with a licensed server program over a given time period. The reported results can be used to determine compliance or non-compliance with the license agreement associated with the program. However, like Christiano, Rivera, *et al.* does not teach or suggest an oversight component having the protective features set forth in independent claim 1.

In addition to the features discussed above, the subject claims disclose that copies of license data can be stored in a backup store. If license data in the license store is determined to be corrupt, the license data can be deleted from the license store, and the backup license data can be checked for validity. If the license data in the backup store is validated, the license can be restored to the license store using the backup copy. Alternatively, if the backup copy cannot be validated, an error message can be displayed and a shutdown of the licensing system can be initiated (see paragraphs [0050] and [0082] of the specification). To this end, independent claim 1 goes on to recite, *a backup store that contains copies of the stored license data, the validation component checks the validity of the copies of the license data in the backup store upon determining that stored license data in the license store is corrupt, restores the corrupt license data from the backup store to the license store upon confirming the validity of the copies, and initiates shutdown of the license enforcement system upon determining that the copies in the backup store are invalid*.

Christiano does not teach or suggest such a backup and restore method. With regard to this aspect, the Examiner again cites a connection diagnostic procedure in Christiano, which is initiated when a license file or server for a designated product cannot be found. According to this diagnostic procedure, in the event that a license file cannot be found on the network in response to a client request, each of a plurality of file servers on the network are polled sequentially to determine whether the server is the correct file server for the designated product. The Examiner maintains that this diagnostic procedure reads on the backup and restore features of independent claim 1, asserting that each of these polled servers represents a backup store for license data. However, these polled servers cannot be said to represent *backup* stores for license data, since there is no corresponding *primary* store for license data in the cited scenario. The cited diagnostic scenario seeks to locate an *original* license file or server on the network, given that an initial request failed to locate the desired file or server on an initial attempt to retrieve the file. This process of locating a correct license file is not initiated by a corruption of original license data, but rather on a failure to locate the license at the expected location on the network.

It therefore cannot be said that the cited license servers represent backup stores for license data. Moreover, there is no mention of creating backup copies of license data in Christiano, or of restoring primary licenses from such backup copies. As such, the cited reference therefore also fails to teach or suggest performing a validation on such backup license data, or initiating a system shutdown when this validation fails. The compliance monitoring system of Rivera, *et al.* also fails to disclose such a license backup and restore procedure.

Similarly, amended independent claim 11 recites, *an oversight component that observes the operation of the monitoring component and restarts the component when it fails to operate properly, the oversight component shuts down the licensed application when the monitoring component cannot be restarted*, and as already discussed, neither Christiano nor Rivera, *et al.* disclose such an oversight component.

The subject claims also disclose that, in addition to controlling the number of users employing a licensed application, the aforementioned license data can enforce policies regarding the appropriate running environment for the licensed application. This can include specifying that the application is not to be run on a workgroup environment. To this end, amended independent claim 11 goes on to recite, *a monitoring component that monitors use of a licensed application by one or more users in accordance with a license agreement**, the license agreement specifying at least that the licensed application is not to be run in a workgroup environment***. Christiano does not teach a license that can specify and enforce a *preferred running environment* for the associated licensed application, but rather is limited only to ensuring that unauthorized users are prevented from using licensed applications. Similarly, Rivera, *et al.* is concerned only with policing the number of concurrent users of a licensed application, and does not contemplate a license that specifies a *preferred operating environment* for an application, much less a license that indicates specifically that a licensed application is to be prevented from running in a workgroup environment.

With further regard to validation of stored license data, the subject claims disclose that the integrity of stored license data can be checked by periodically comparing the stored data with the corresponding license data in the backup store. Specifically, a license key and hardware ID associated with the license data in the data store can be compared periodically with that in the backup store to ensure that the stored license has not been corrupted or tampered with (see, for example, paragraph [0050], lines 1-9 of the specification). Thus, the copy of the license data stored in the backup store is multi-functional, in that it facilitates periodic validation of the primary license data stored in the data store, and acts as a backup from which the primary license can be restored should the primary data become corrupted. In particular, amended independent claim 20 recites, *a license store that receives license data from a license component associated with a licensed application, the license data includes at least a license key and a hardware ID; a backup store that receives a copy of the license data for backup storage; [and]* ***a validation component that compares the license key and hardware ID stored in the backup store with those in the license store at regular time intervals to ensure that the license data in the license store has not been corrupted****.*

As noted above, Christiano does not teach or suggest storing a backup copy of license data in a backup store. Consequently, the cited reference also fails to disclose periodically comparing a license key and hardware ID associated with this backup copy with the primary license data stored in a license store in order to confirm validity. Indeed, Christiano does not contemplate any manner of periodic verification of a stored license, much less *via* comparison with a backup copy of the license as set forth in amended independent claim 20. Rivera, *et al.* does not remedy this deficiency, since that cited reference does not consider methods for checking *validity* of a license file.

Amended independent claim 20 further recites, *an oversight component that observes the operation of the monitoring component and restarts the component when it fails to operate properly, the oversight component shuts down the licensed application when the monitoring component cannot be restarted*, and as discussed *supra*, neither Christiano nor Rivera, *et al.* teach or suggest such an oversight component.

Disclosing additional license functionality, amended independent claim 29 recites, *monitoring license data in a data store corresponding to a licensed application, wherein* ***the licensed data includes at least a specification of at least one second application that is not to be run in conjunction with the licensed program; monitoring use of the licensed application on a system****.* Neither cited reference teaches a license specifying one or more second applications that should not be run in conjunction with the license program. Rather, as already noted, Christiano, and Rivera, *et al.* only contemplate licenses that prevent unauthorized use of the licensed application, and do not teach an additional enforcement of restrictions on concurrently running applications.

Amended independent claim 29 goes on to recite, *determining that monitoring of the license data has stopped; restarting the monitoring upon determining that the monitoring has stopped; and shutting down the licensed application when the monitoring cannot be restarted.* As discussed above, neither cited reference teaches or suggests such oversight functionality over license monitoring.

Additionally, amended independent claim 40 recites, *installing the license component on a computer, wherein installing the license component includes storing license data in a license store, the license data including a license key and a hardwire ID identifying the computer on which the license component is installed; storing a copy of the license data in a backup store;* ***retrieving the license key and hardwire ID from the backup store at periodic times; [and] comparing the retrieved license key and hardware ID with the corresponding license key and hardware ID in the license store at the periodic times***. Christiano and Rivera, *et al.* do not disclose this technique for periodic license validation, as discussed above. Amended independent claim 40 goes on to recite, *checking the validity of the copy of the license data in the backup store; restoring the license data from the backup store to the license store when it is determined that the copy of the license data in the backup store is valid; and initiating shutdown of the computer system when it is determined that the copy of the license data in the backup store cannot be validated.* As already noted, neither cited reference teaches or suggests a backup and restore method whereby, in the event of corruption of a primary license, a stored backup license is validated prior to performing a restore operation, and a shutdown is initiated if the backup license fails to validate. Indeed, neither Christiano nor Rivera, *et al.* disclose the use of backup licenses, and as such fail to contemplate the backup validation procedure disclosed in amended independent claim 40.

Moreover, new claim 44 recites*, the validation component periodically checks the validity of the license data in the license store by comparing a license key and hardwire ID from the backup store with the corresponding license key and hardware ID in the license store.* The cited references fail to teach such periodic checks, as already discussed.

As can be seen, the present claims teach a number of protocols for license validation and compliance monitoring not disclosed in Christiano or Rivera, *et al.*, including periodic comparison of a primary license with a backup copy of the license to detect corruption or tampering, restoration from this backup license in the event of corruption, system shutdown when it is determined that both the primary and the backup licenses are invalid, and regular verification that license compliance is being properly monitored using oversight functionality. None of these aspects are taught or suggested by the cited references.

In view of at least the foregoing, it is respectfully submitted that Christiano and Rivera, *et al.*, individually or in combination, do not teach or suggest each and every feature of independent claims 1, 11, 20, 29, 40 (and all claims depending there from), and as such fail to make obvious the present invention. It is therefore requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP494US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,
AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
127 Public Square
57th Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731